DigiKnow

CYBER SECURITY DEPENDS ON YOU

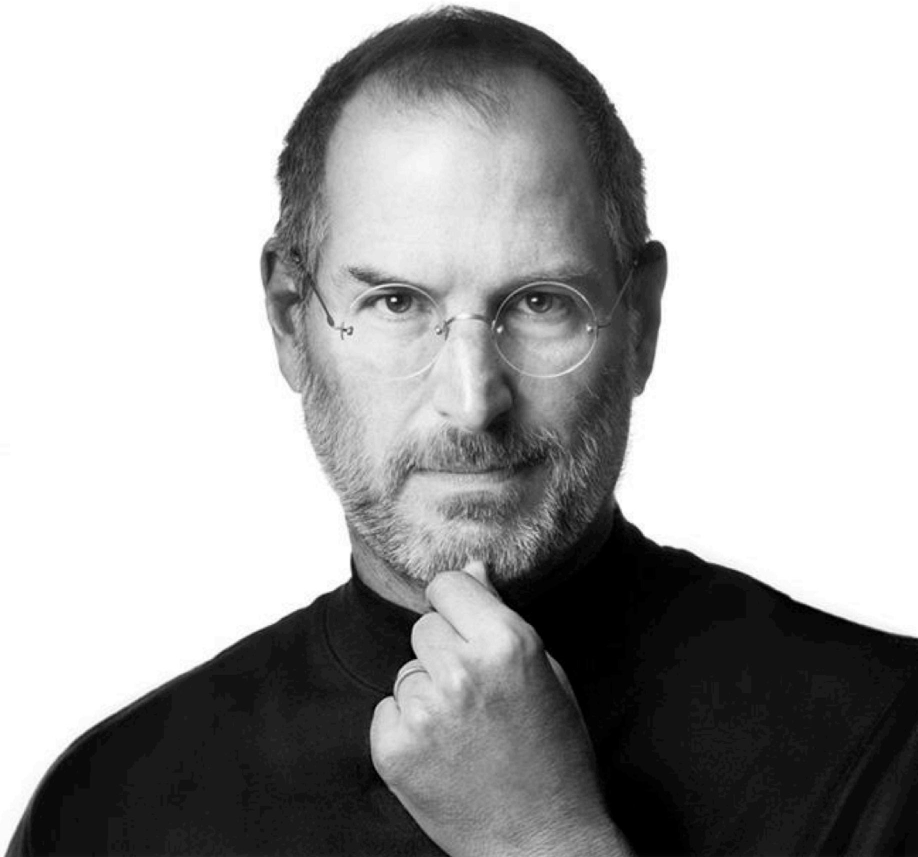
2016 SECURE DELAWARE WORKSHOP

Security Report: 100% Chance of Clouds

Mark Weatherford
vArmour
Chief Cybersecurity Strategist

"People who know what their talking about don't need PowerPoint."

- Steve Jobs



Cloud computing is…“a sea change - a deep and permanent shift in how computing power is generated and consumed. It’s as inevitable and irreversible as the shift from steam to electric power in manufacturing, which was gaining momentum in America about a century ago.”

- Andrew McAfee, Harvard Business Review, November 2011

Cloud-based products and services are growing across the board and more than 86% of all workloads will be processed by cloud data centers by 2019.

- Cisco Cloud Index 2015

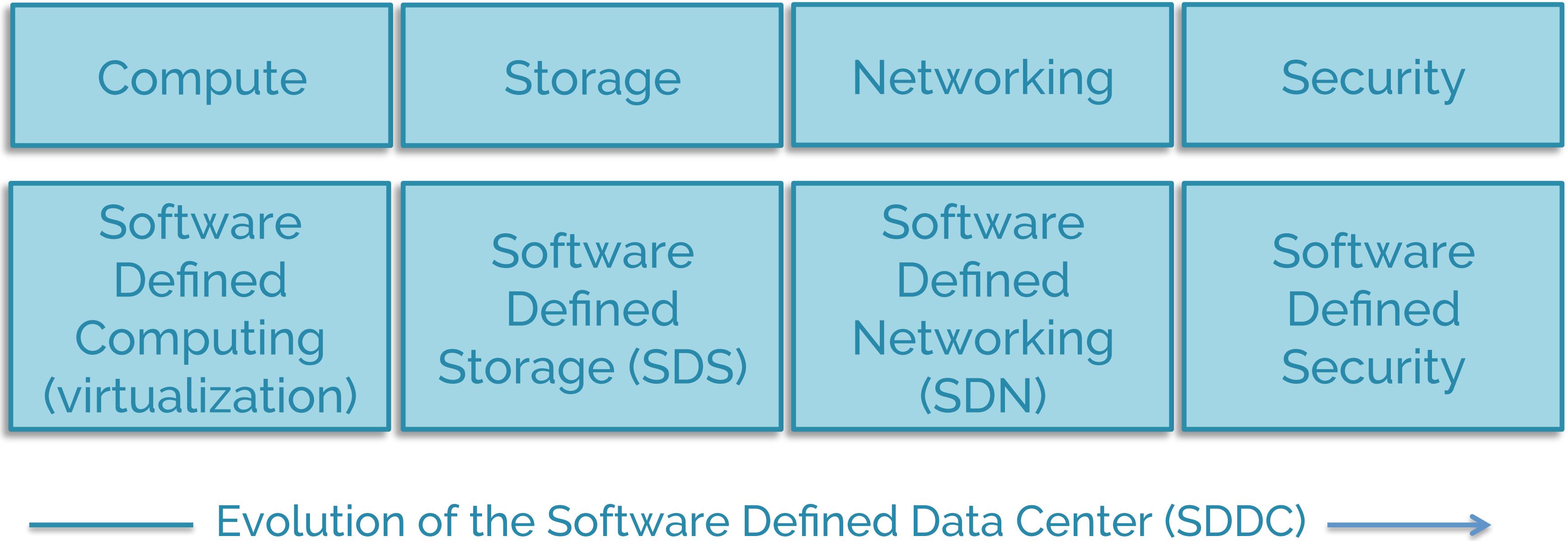
Bezos' Law: *"Over the history of Cloud Computing, a unit of computing power price is reduced by 50 percent approximately every three years."*

- Greg O'Connor, CEO, AppZero

The IT world is shifting from physical infrastructure to digital and software-defined technologies…

And the shift is having a profound effect on the core infrastructure of the data center and the cloud

Software Defined Everything (SDx)



Compute

Storage

Networking

Security

Software Defined Computing (virtualization)

Software Defined Storage (SDS)

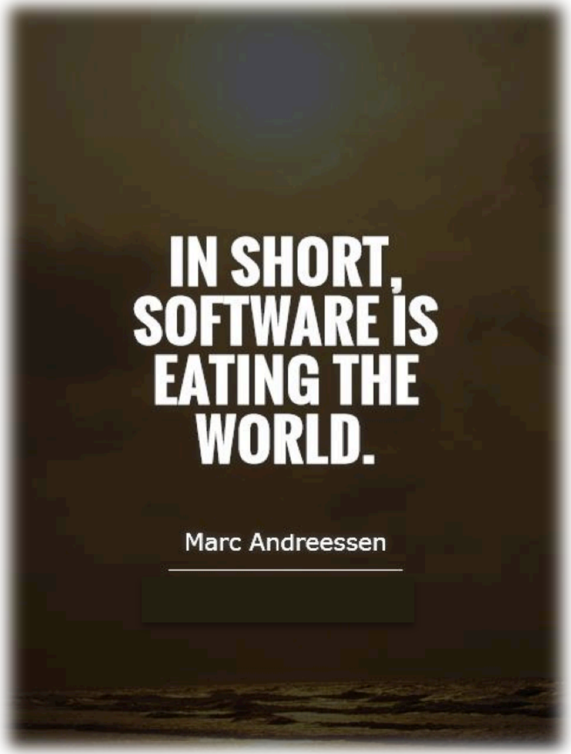
Software Defined Networking (SDN)

Software Defined Security

Evolution of the Software Defined Data Center (SDDC)

“The era of separating traditional industries and technology industries is over, and those who fail to adopt right now will soon find themselves obsolete.”

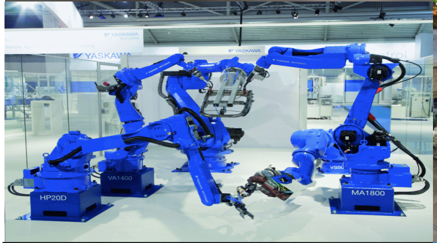
- Forbes.com

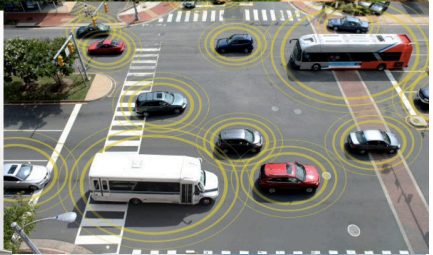


IN SHORT, SOFTWARE IS EATING THE WORLD.

Marc Andreessen

New products and services depend on the cloud





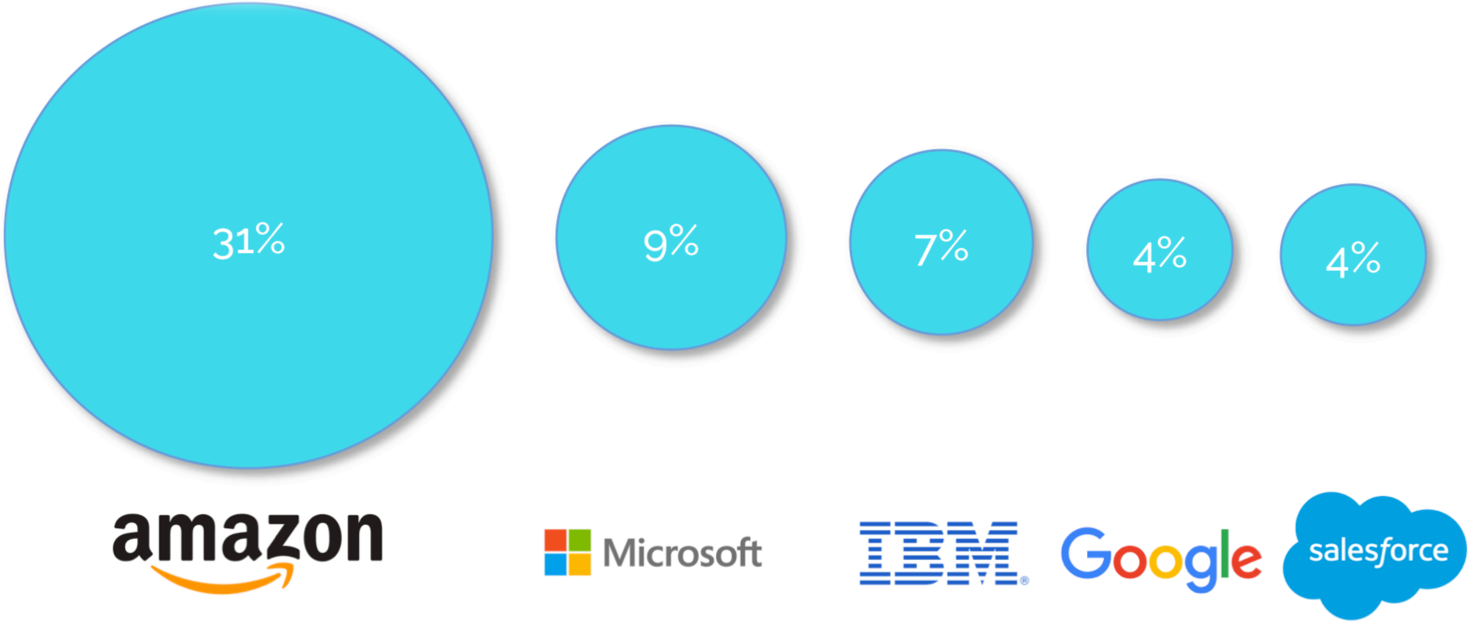
RECIPE SEARCH BY INGREDIENT

Search Results for.

Main Ingredient

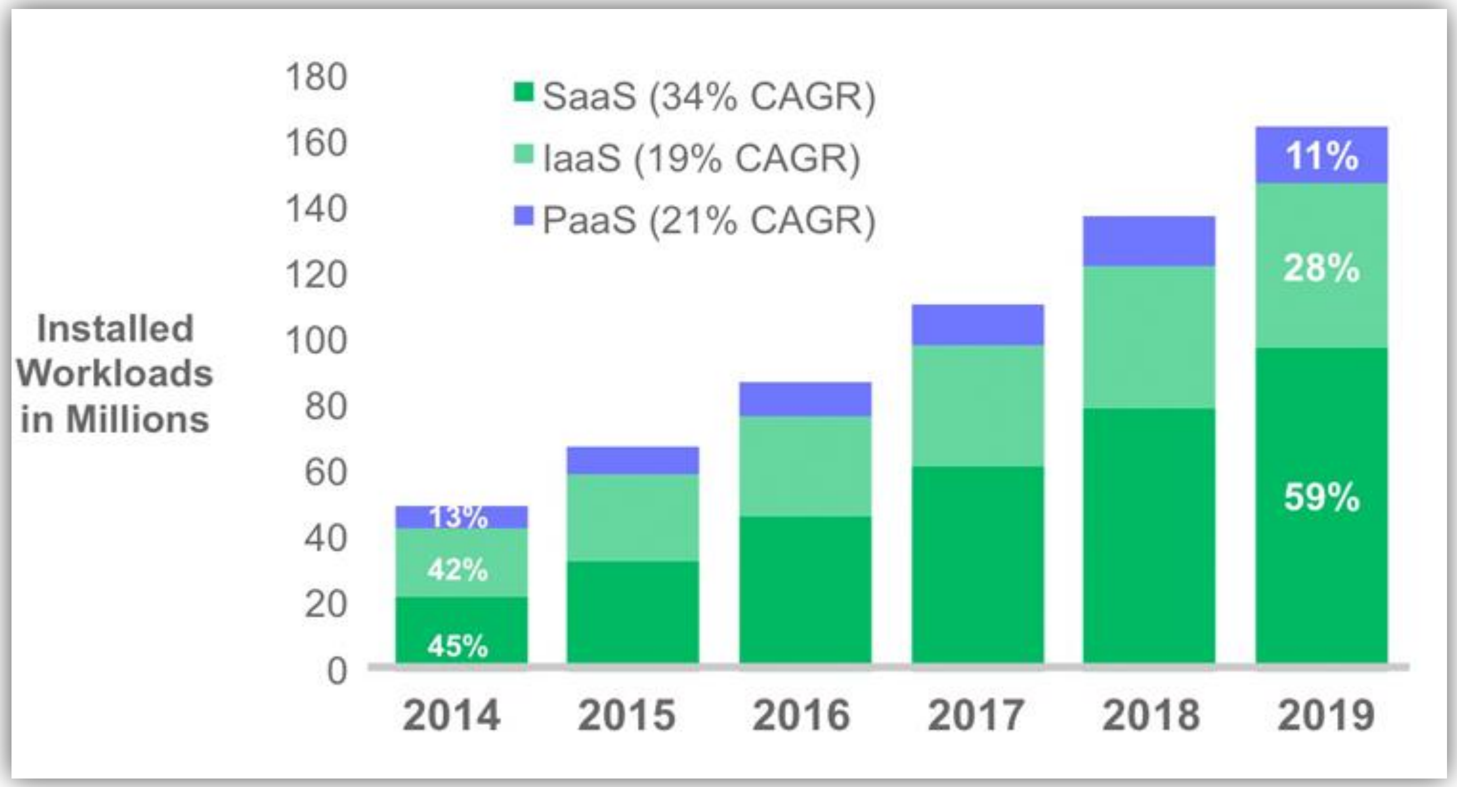
Top 5 cloud infrastructure service providers

Worldwide cloud infrastructure services market share in 2015
includes SaaS, IaaS, PaaS, private and hybrid cloud services



Source: Synergy Research Group

SaaS is the most highly deployed cloud service



Cisco Global Cloud Index 2014-2019

IT and business operations are moving

- 85.9 percent of web content management
- 82.7 percent of communications
- 80 percent of app development
- 78.9 percent of disaster recovery
- 81.3 percent of sales and marketing
- 79.9 percent of business analytics
- 79.1 percent of customer services
- 73.5 percent of HR & Payroll activities

Wikibon/North Bridge Ventures 2015 Future of Cloud Computing Survey

CAPEX vs OPEX

- Static investment vs. dynamic investment
- Lower costs, more flexibility and easier to scale
- Less dependency on legacy infrastructure
- Pay for only the capacity you need, when you need it
- Transfer some of the IT risk to the cloud provider

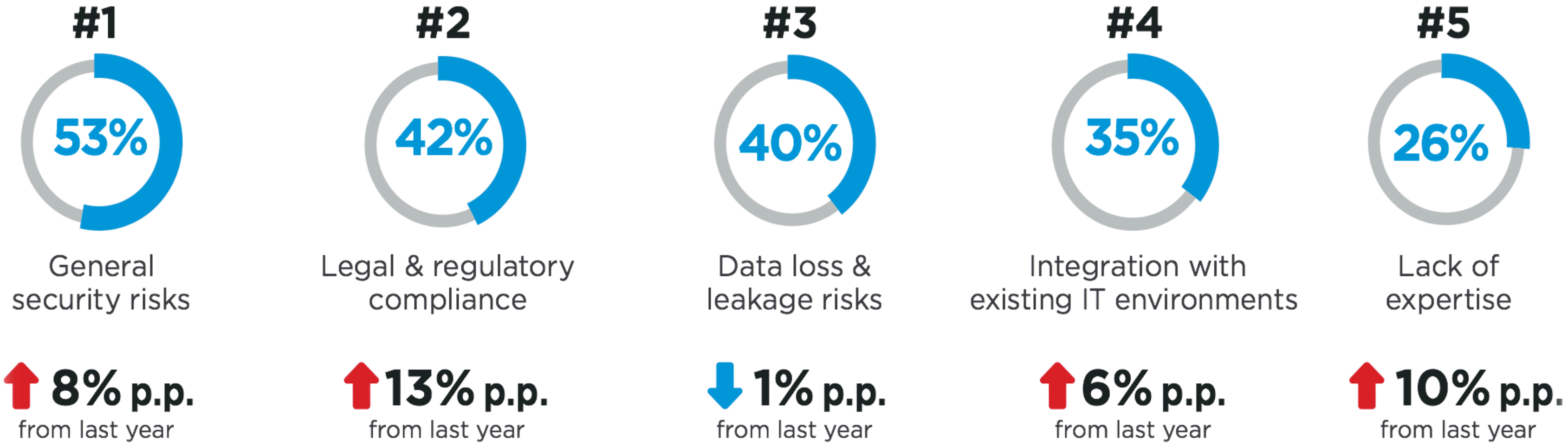
But … is it safe?

While cost continues to be the primary driver for moving to the public cloud, the top inhibitor is still….

Security

https://www.veritas.com/news-releases/2016-06-28-state-of-the-hybrid-cloud-research.html

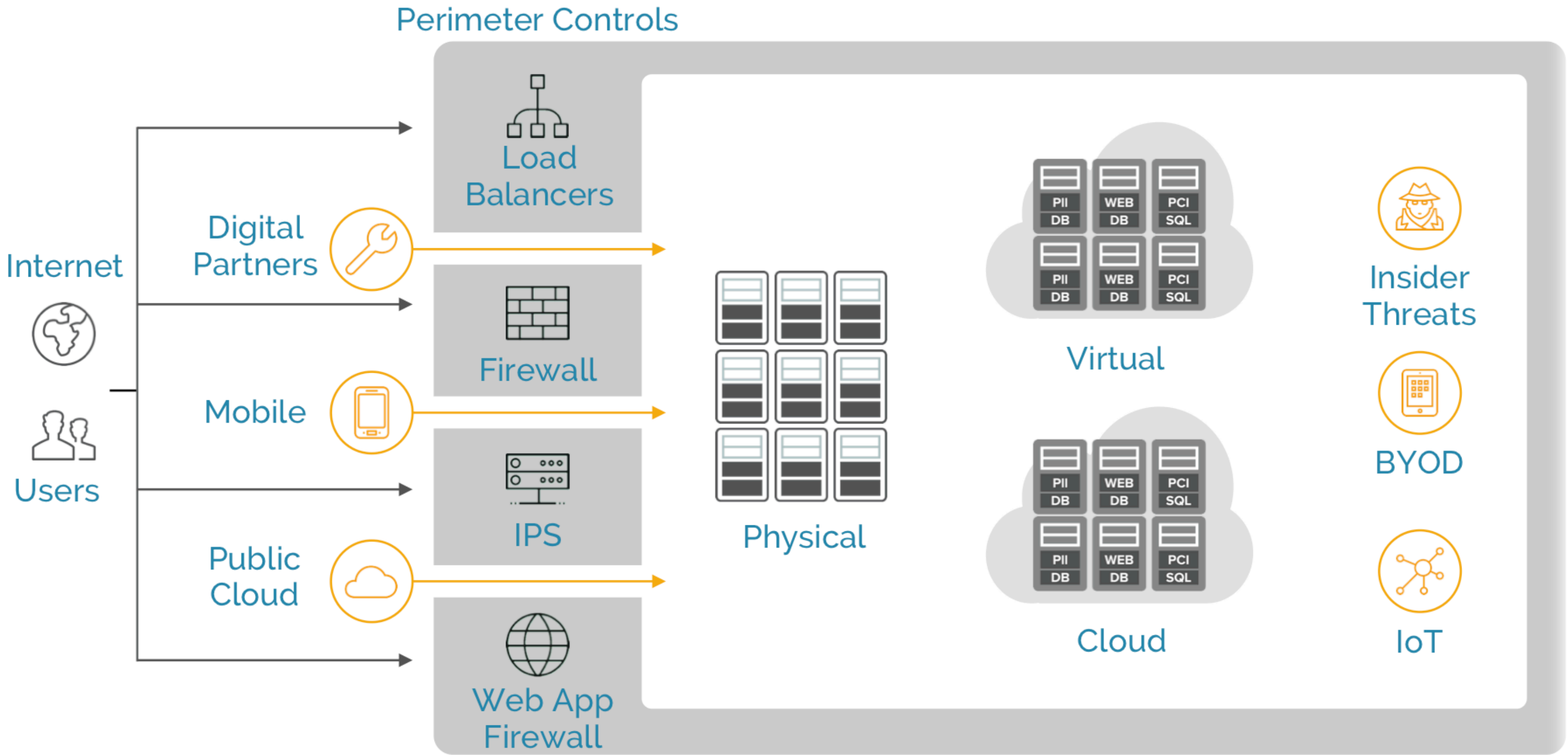
Barriers to cloud adoption



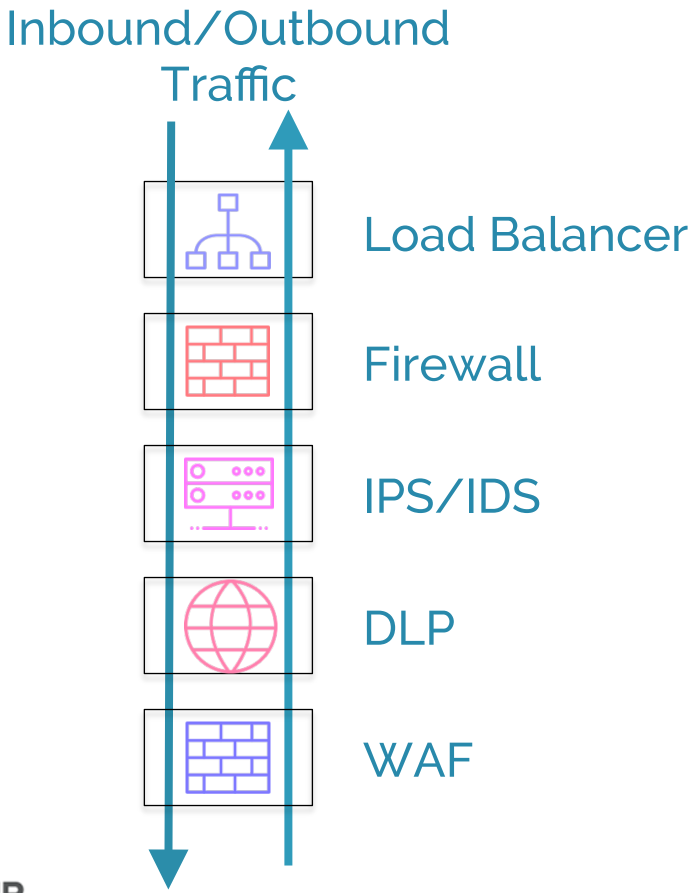
#1	#2	#3	#4	#5
53%	42%	40%	35%	26%
General security risks	Legal & regulatory compliance	Data loss & leakage risks	Integration with existing IT environments	Lack of expertise
↑ 8% p.p. from last year	↑ 13% p.p. from last year	↓ 1% p.p. from last year	↑ 6% p.p. from last year	↑ 10% p.p. from last year

http://www.crowdresearchpartners.com/wp-content/uploads/2016/05/Cloud-Security-Report-2016.pdf

The perimeter is dead, long live the cloud



80/20 rule for data center and cloud traffic



Inbound/Outbound Traffic

Load Balancer

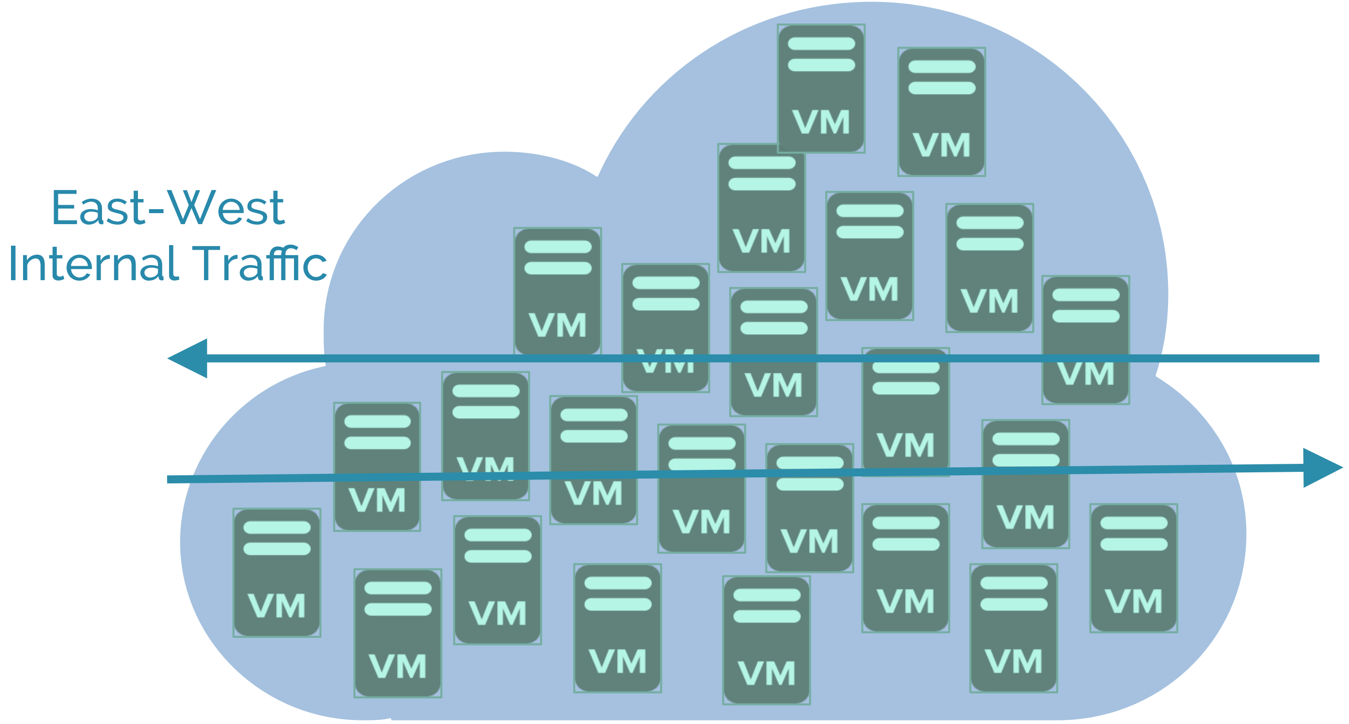
Firewall

IPS/IDS

DLP

WAF

Only 20% of traffic is inspected by traditional perimeter security solutions



80% of data center traffic isn't screened by perimeter controls for suspicious/ unauthorized behavior or application misuse.

…we're blind inside the cloud

Most companies aren't instrumented for east-west traffic visibility inside their virtual data centers and cloud so they see very little of the actual data communications

Security challenges and opportunities

Separation of assets: Micro-Segmentation

Visibility and monitoring of applications and users

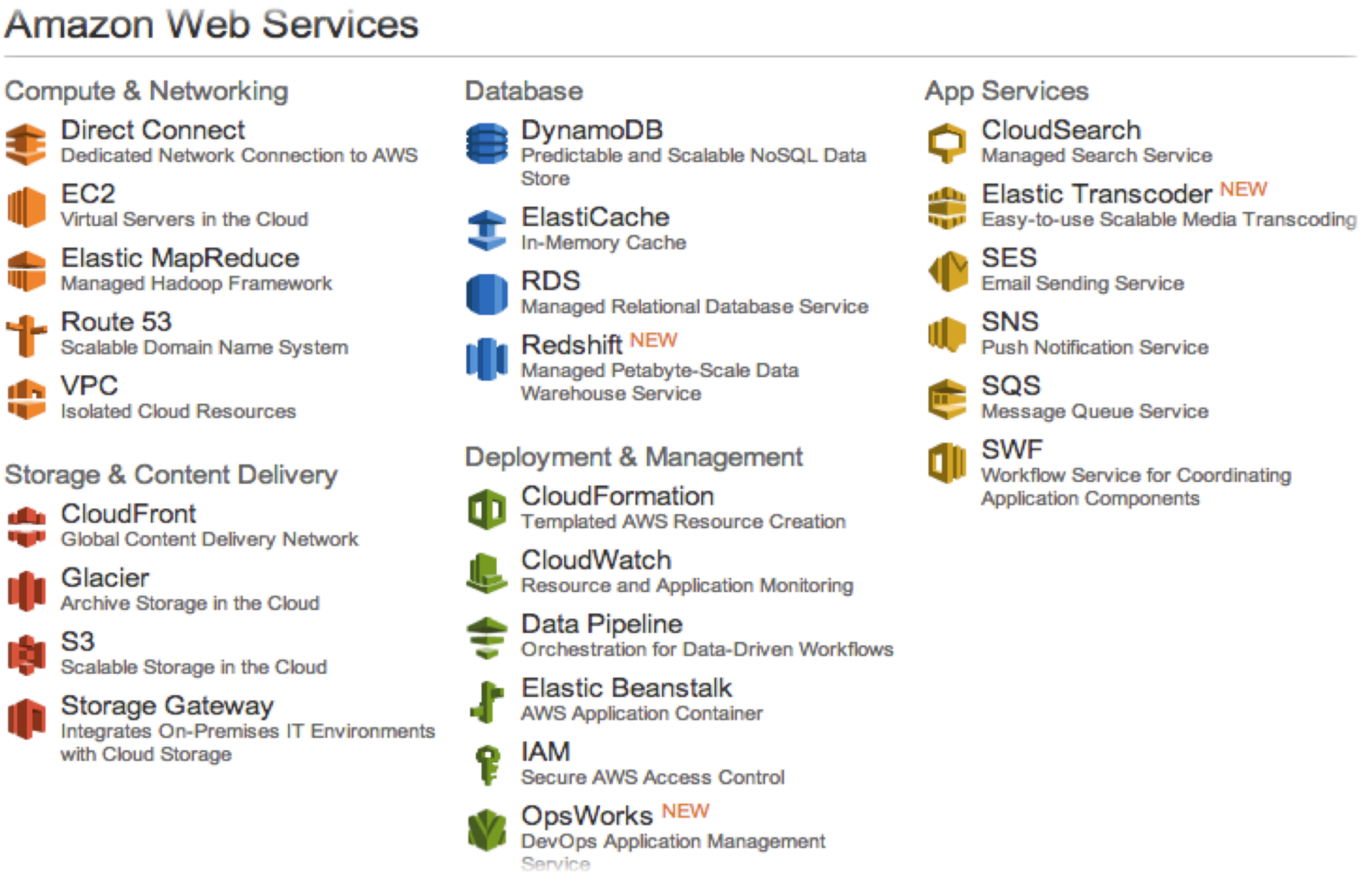
Detecting and mitigating APTs and insider threats

Investigating security incidents Incident Response and Forensics

Managing security across Multi-Cloud Environments

Shadow IT

The AWS shadow IT challenge



Amazon Web Services

Compute & Networking

Direct Connect
Dedicated Network Connection to AWS

EC2
Virtual Servers in the Cloud

Elastic MapReduce
Managed Hadoop Framework

Route 53
Scalable Domain Name System

VPC
Isolated Cloud Resources

Storage & Content Delivery

CloudFront
Global Content Delivery Network

Glacier
Archive Storage in the Cloud

S3
Scalable Storage in the Cloud

Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage

Database

DynamoDB
Predictable and Scalable NoSQL Data Store

ElastiCache
In-Memory Cache

RDS
Managed Relational Database Service

Redshift NEW
Managed Petabyte-Scale Data Warehouse Service

Deployment & Management

CloudFormation
Templated AWS Resource Creation

CloudWatch
Resource and Application Monitoring

Data Pipeline
Orchestration for Data-Driven Workflows

Elastic Beanstalk
AWS Application Container

IAM
Secure AWS Access Control

OpsWorks NEW
DevOps Application Management Service

App Services

CloudSearch
Managed Search Service

Elastic Transcoder NEW
Easy-to-use Scalable Media Transcoding

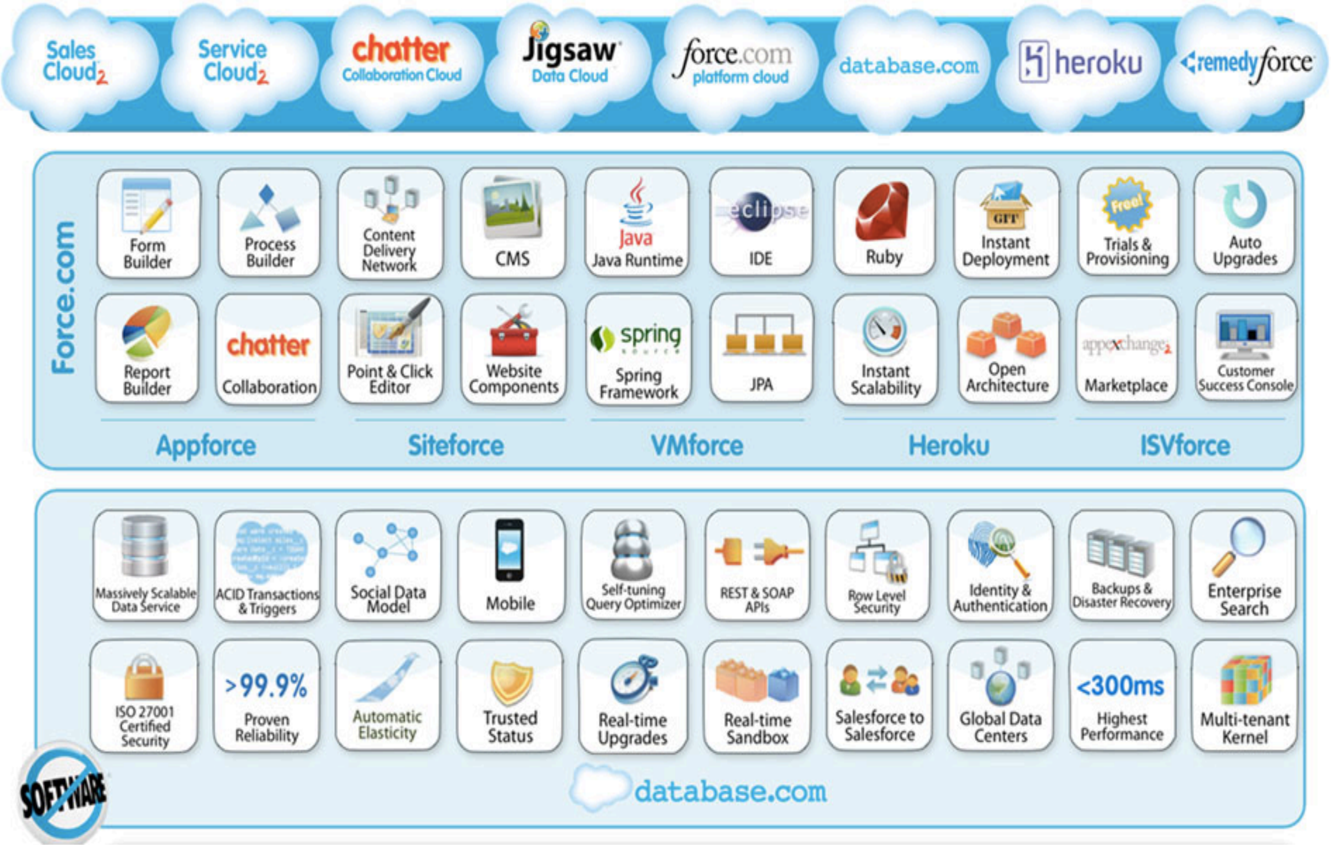
SES
Email Sending Service

SNS
Push Notification Service

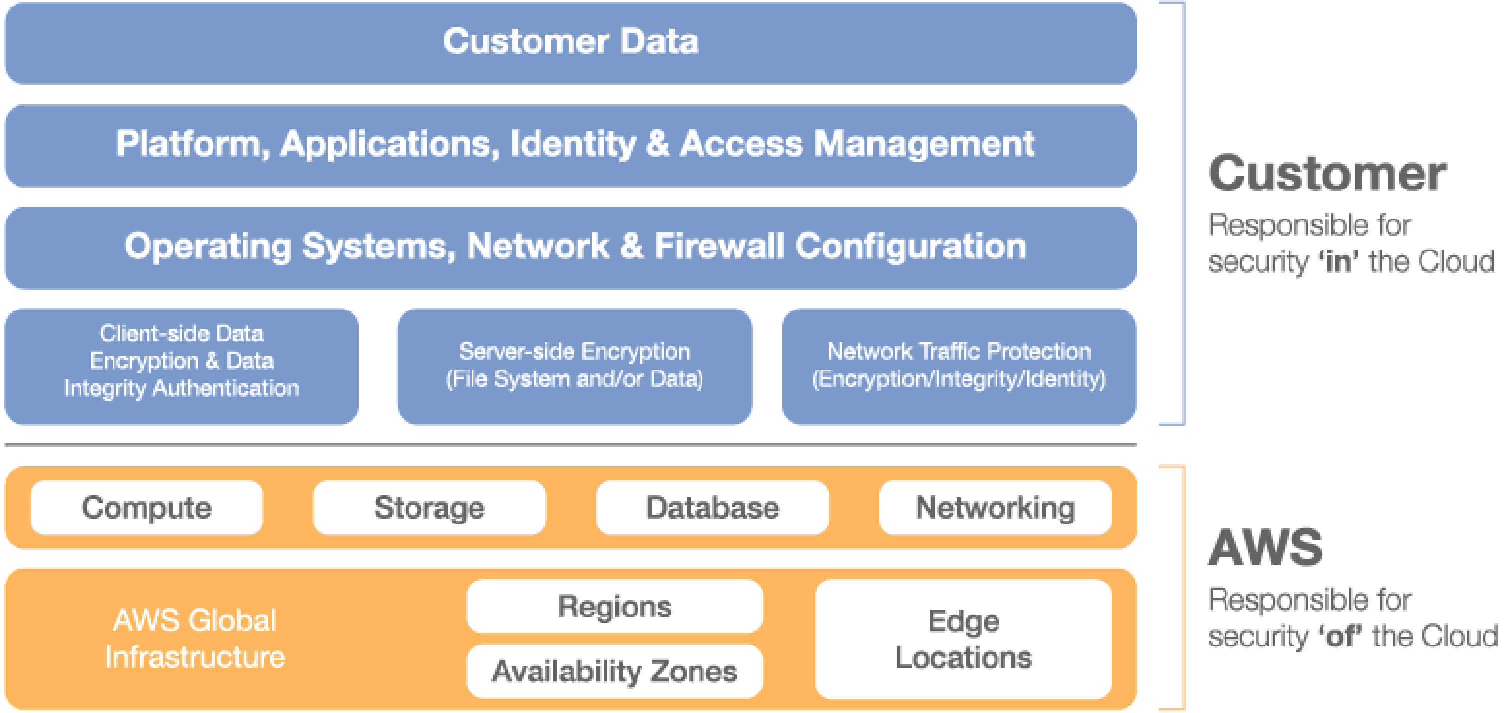
SQS
Message Queue Service

SWF
Workflow Service for Coordinating Application Components

The Salesforce shadow IT challenge



AWS shared responsibility model



Customer Data

Platform, Applications, Identity & Access Management

Operating Systems, Network & Firewall Configuration

Client-side Data Encryption & Data Integrity Authentication

Server-side Encryption (File System and/or Data)

Network Traffic Protection (Encryption/Integrity/Identity)

Compute

Storage

Database

Networking

AWS Global Infrastructure

Regions

Availability Zones

Edge Locations

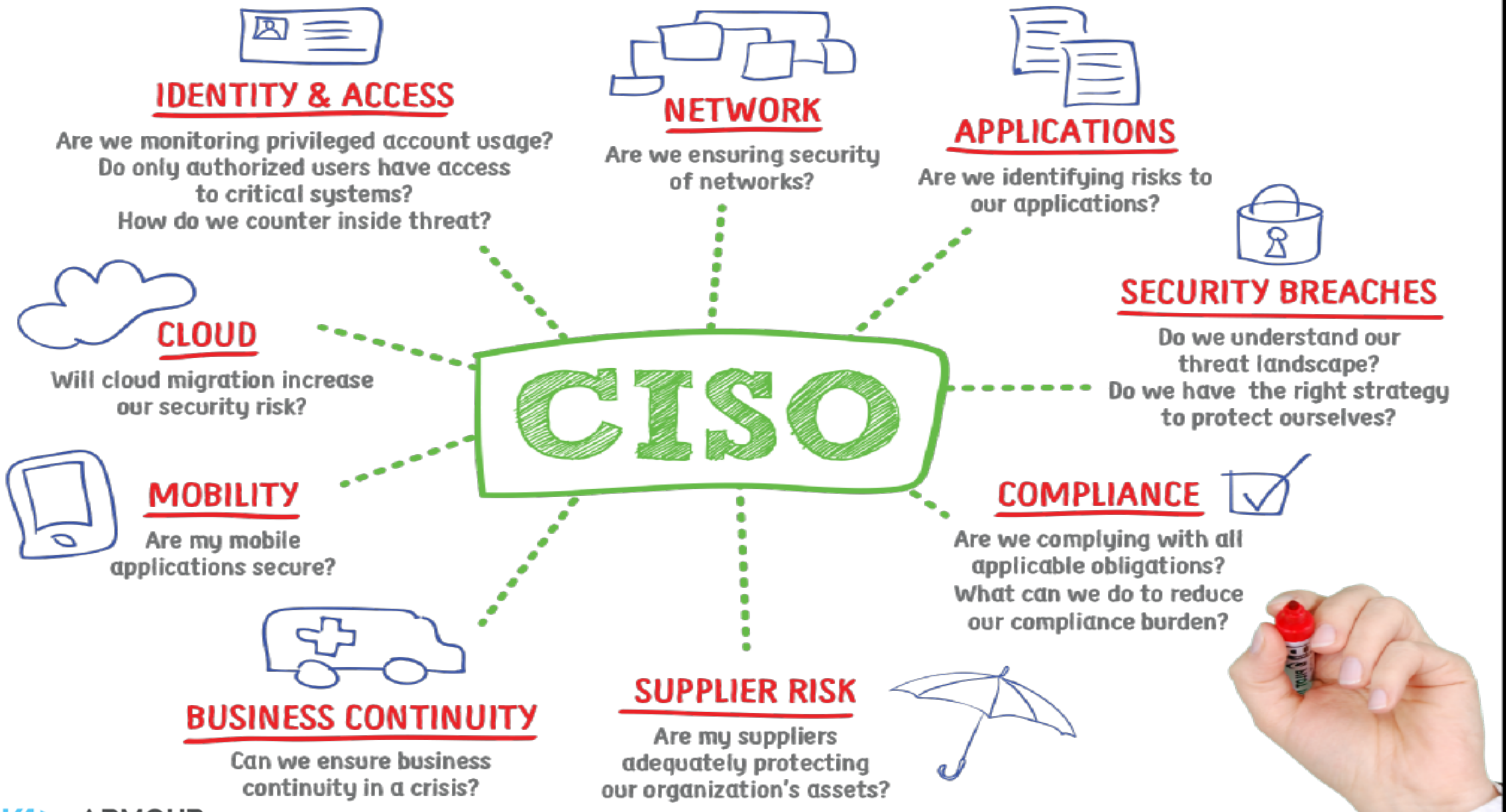
Customer

Responsible for security **'in'** the Cloud

AWS

Responsible for security **'of'** the Cloud

Source: Amazon, Evercore ISI Research



CISO

IDENTITY & ACCESS

Are we monitoring privileged account usage?
Do only authorized users have access to critical systems?
How do we counter inside threat?

NETWORK

Are we ensuring security of networks?

APPLICATIONS

Are we identifying risks to our applications?

SECURITY BREACHES

Do we understand our threat landscape?
Do we have the right strategy to protect ourselves?

COMPLIANCE

Are we complying with all applicable obligations?
What can we do to reduce our compliance burden?

SUPPLIER RISK

Are my suppliers adequately protecting our organization's assets?

BUSINESS CONTINUITY

Can we ensure business continuity in a crisis?

MOBILITY

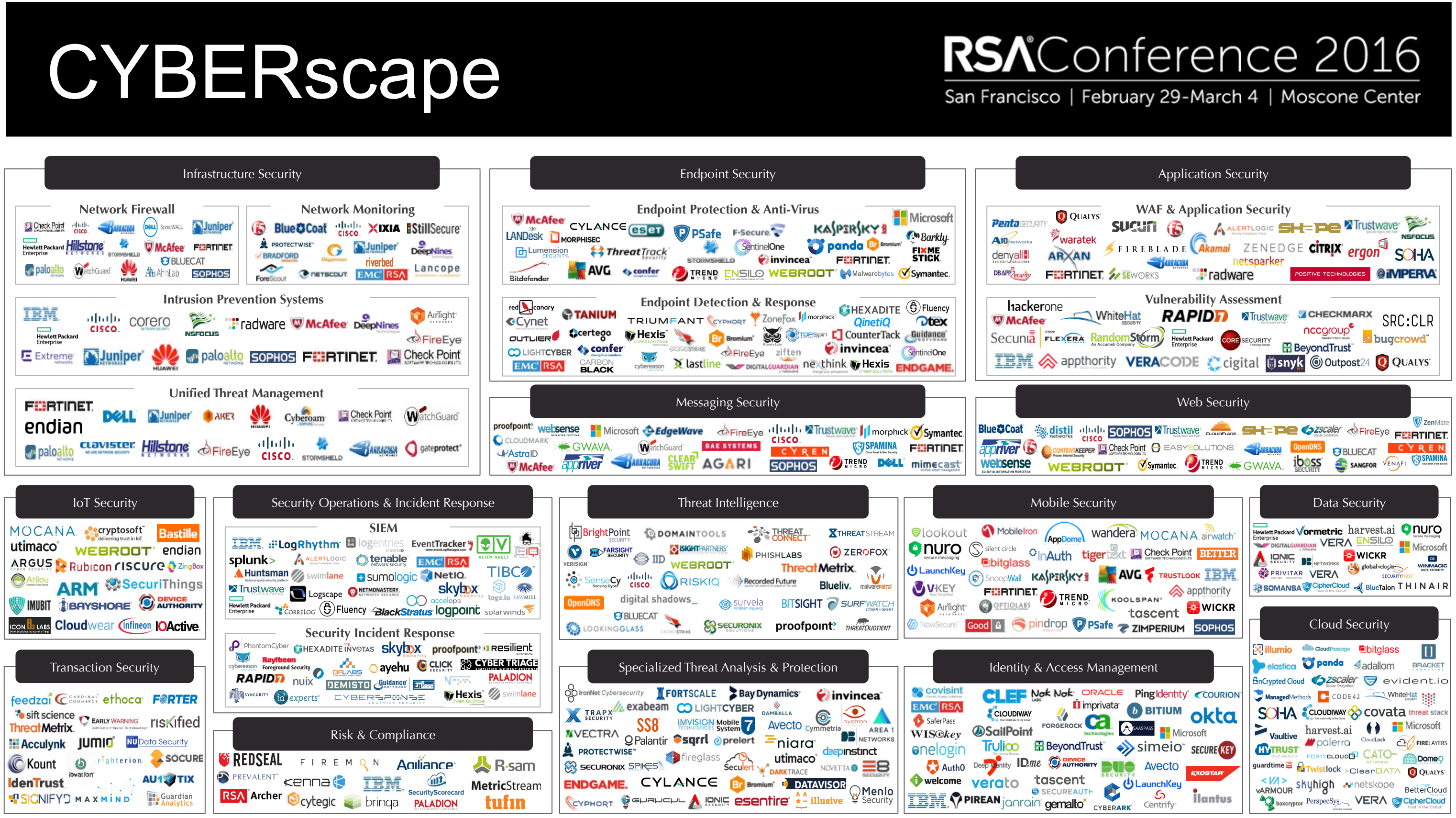
Are my mobile applications secure?

CLOUD

Will cloud migration increase our security risk?

<vARMOUR

Complexity is the enemy…


CYBERscape
RSAConference 2016
San Francisco | February 29-March 4 | Moscone Center
Infrastructure Security
Network Firewall
Network Monitoring
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Protection & Anti-Virus
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Messaging Security
Web Security
IoT Security
Security Operations & Incident Response
SIEM
Security Incident Response
Threat Intelligence
Mobile Security
Data Security
Cloud Security
Transaction Security
Risk & Compliance
Specialized Threat Analysis & Protection
Identity & Access Management

Source: Momentum Partners.

The cloud is a catalyst for better security

Adoption of cloud applications and services is accelerating - not because you don’t know what or how to do it but:

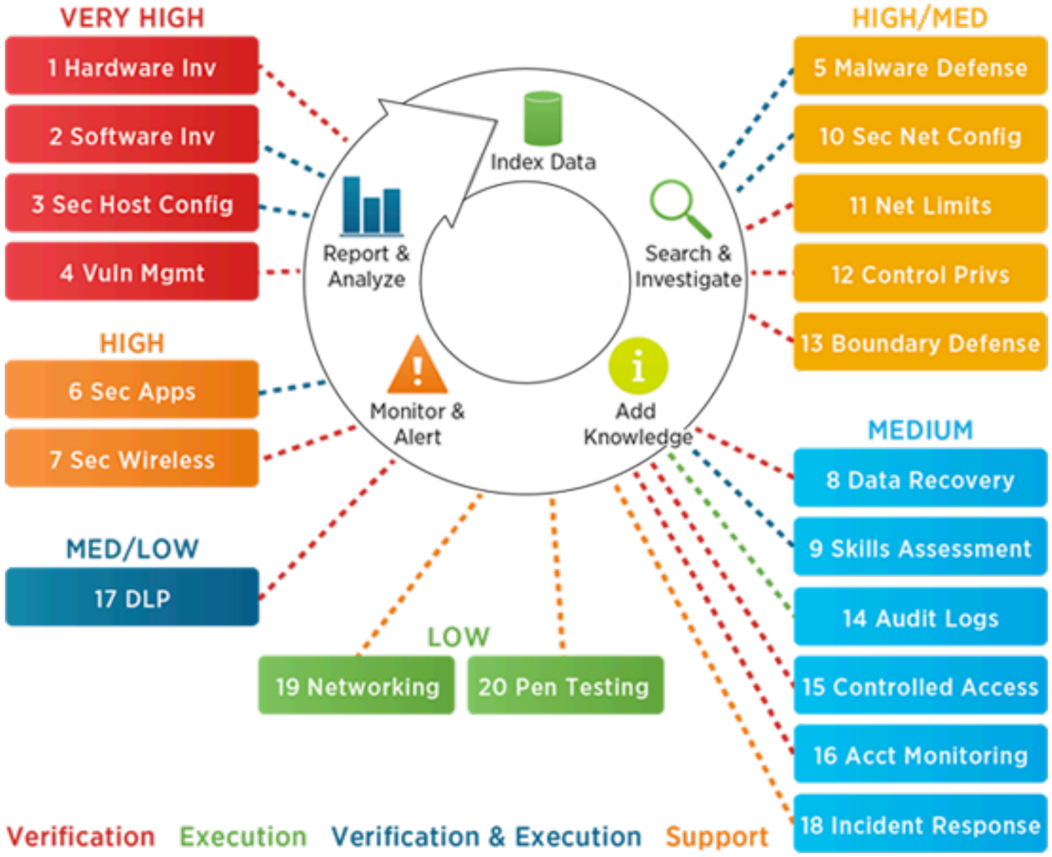
- The economic advantages are profound
- Provides anywhere/anytime access
- Offers high reliability and automatic backups
- Better resourced, with around-the-clock support
- Technical skills – they have what you don’t have and can afford it
- Cloud providers are highly incentivized to deliver security - they are more paranoid than you

Asking the right questions is key…

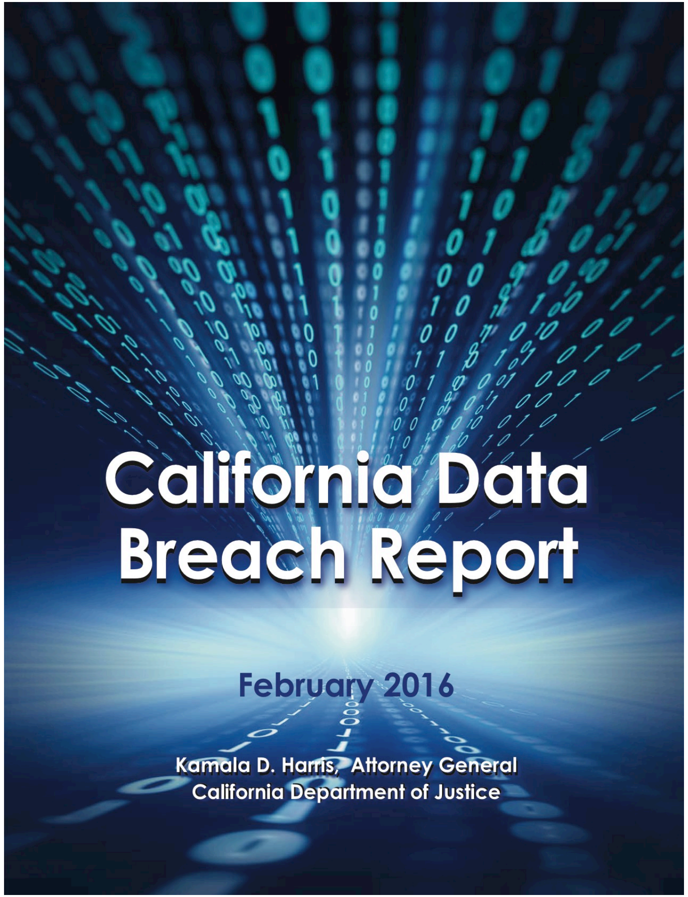
1. What kinds of data centers (Tier 1/2/3) does the cloud provider use?
2. What is your cloud provider's disaster recovery plan?
3. What compliance certifications does the cloud provider have?
4. What are the cloud provider's encryption policies?
5. How is my data isolated from other clients' data?
6. Can I use my existing IAM software to control cloud access?
7. How is activity in my account monitored and documented in log files?
8. Can I visit a data center and do my own inspection?
9. What must I know in case I decide to change cloud providers?

- Stephan Lawton in Tom's IT Pro

Top 20 Critical Controls



Top 20 Critical Controls … a bridge too far?

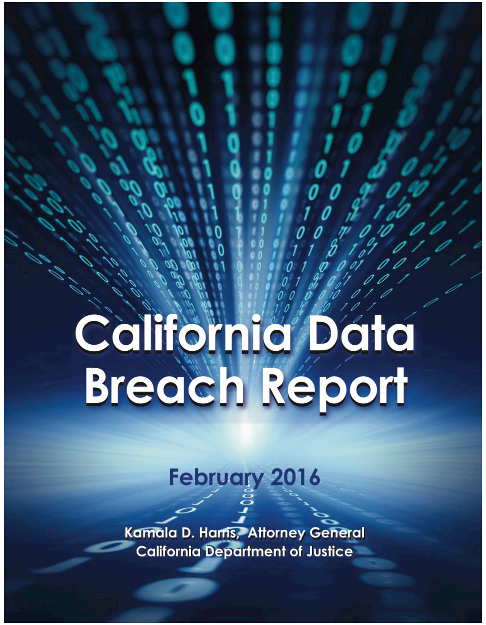


California Data Breach Report

February 2016

Kamala D. Harris, Attorney General
California Department of Justice

Top 20 Critical Controls … a bridge too far?



California Data Breach Report

February 2016

Kamala D. Harris, Attorney General
California Department of Justice

Recommendations

1) The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement *ALL* (emphasis mine) the Controls that apply to an organization's environment constitute a lack of reasonable security.

There's an old Soviet saying:

- If you think it, don't say it.
- If you say it, don't write it.
- If you write it, don't be surprised.

Dan Kaminsky's Blog

THE ENEMY ISN'T HACKERS IT'S APATHY

mark@varmour.com